REMARKS

Claims 55 – 85 are currently pending in this response. Claims 55 - 85 are rejected. Claims 55, 56, 65, 68, 73 – 75, 78 – 82 and 85 are amended in this response.

Amendments to claims 56, 65, 68, 73 – 75, 78, 79, 82 and 85

The above claims are amended to deal with clarity and antecedent issues that made themselves apparent to applicant while preparing this response.

Claim Rejections – 35 USC 103

The Examiner rejected claims 55 – 85 under 35 USC 102(e), as being obvious over Helgeson et al. US Patent No. 6643652, and associated application No 2002/0073236, in view of Brown, US Patent Application No. 2003/0061317.

Applicant first provides a non-limiting overview of the subject matter of the present embodiments for the benefit of the Examiner.

The present embodiments allow a user at a remote device to interact with a first object on a first host, and, through that first object, to interact with a second object on a second host. This interaction is carried out independently of other users who are able to interact with the same objects at the same time.

For example the first object on the first host may be a table of weather readings taken from weather stations around the world. The second object may be an interactive weather map that knows how to take numbers from a table, assign them to the correct places on the map and then display local weather conditions in various places.

The remote user now accesses the table, the first object, and sends it to the second object. As he accesses the first object the table identifies itself as being from the first host and belonging to the remote user. The data then arrives at the second host where it is applied to the interactive map object. The interactive map object can deal with data from anywhere as long as it is in a suitable format. However the two above identities are preserved with the interaction so that the resulting interactive map retains the identity of the first host (where the data came from) and the identity of the remote user – so that any results are clearly associated with that particular user and do not interfere with any other users.

Thus the particular remote user obtains his weather map with his data, and without interfering with other users.

The remote user obtains his weather display without ever hosting a weather map object on his own computer, and furthermore can do so by providing information that was never hosted on his own computer.

The following is a further example of what the invention is able to do. In the previous example the server identity, though present, was not fully taken advantage of. In the following, the user has a list of weather data on an Internet weather service. This is his *private* data. It is noted that even if each datum itself is public, the set of data *as a whole* is private.

The user wishes to map the data. He has subscribed to a mapping service. He drags the icon representing his list of weather data, and drops it on the mapping icon.

What "really" happens is that an object on the mapping host suddenly gets a message saying that it has been dropped on by some object. The mapping object sends the object a message saying "give me your data".

The weather object suddenly gets a message from some object asking for its private data. Should it give it? First, being subscription only, the weather object wants to know who is doing the asking. It sees from the user ID in the message who the user is. It sees from the user ID of the mapping object who owns that object. Are these users permitted to access this data? Yes. It knows this, in part, by checking its own ID. Second, is this host trustworthy? Perhaps it is falsifying the user? It checks that its user has authorized this host to receive its private data. It sends the data. Prior art systems which do not insist on the pairing of the user and server data are unable, at the level of a second object in a chain, as above, to authenticate the original user.

Another possible use of the host ID is to ask for additional information before responding. Normal message protocol is request-response. But *before* giving its response, the weather object might want to initiate a request of its own to the mapping object (for example, to ask what kind of object is it?) before responding. For this it needs to know which host to send the message to.

As per features in the dependent claims, the two different objects can be represented by icons on his desktop so that the remote user actually drags an icon of the weather table to the icon of the weather map in order to generate his private weather map.

The above is a general introduction. Applicant has amended the independent claims to more particularly point out the invention for which protection is required.

Applicant has specifically limited the claims to host identities of two servers, wherein a software object at one server is manipulated and wherein an interaction is requested with the software object at the second server, the identity of the first host and the remote user being preserved with the interaction at the second host.

Thus claim 1 recites:

"wherein said first and said second identity arrangements enable a plurality of remote entities to access said enablement data of a first of said hosted software objects simultaneously, said respective host and second identity arrangements being preserved with said access such that manipulations of said software object by any one of said remote entities is independent of manipulation of said remote object by any other remote entities, and wherein each respective second, relationship, identity is transferrable with correspondingly independently manipulated data to another one of said hosting servers for a second manipulation with a further software object at said another hosting server, said second manipulation preserving said second, relationship, identity, thereby allowing said respective remote entity to retain a relationship with said further software object after manipulation thereof through said first software object."

No such feature of preservation of a first and second identity arrangement stored with a first software object to allow independent manipulation thereof is taught in either Helgeson or Brown.

Even if it were, there is no teaching of storing the identity of the host together with the identity of the remote user both together in conjunction with the interaction at this first software object.

Even if it were there is no teaching that interaction with a second object is possible *through* the first object.

Even if it were, there is no teaching that the first and second identities *set up at the first object* should be preserved during an *interaction* with the *second* object, which interaction is carried out *through* the first object.

It is therefore submitted that the features taught in combination in claim 1 are neither taught nor hinted at in either Helgeson or Brown.

Equivalent amendments have been made to independent claims 80 and 81, which are believed to be inventive for the same reasons.

Conclusion

All the matters raised by the Examiner are believed to have been dealt with.

Claims 55, 80 and 81 are believed to be inventive over the combination of Hegelson and Brown.

All the matters raised by the Examiner have been dealt with and allowance of the application is respectfully awaited.

Respectfully submitted,

Martin D. Moynihan
Registration No. 40,338

Date: June 16, 2009

Enclosures:

- Request for Continued Examination (RCE)